IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 5029
Buer, *et al*	Art Unit: 2136
Application No.: 10/617,465	Examiner: Carlton Johnson
Filed: July 11, 2003	Atty. Docket: 2875.0370001
For: **Security Association Updates in a Packet Load-Balanced System**	

Brief on Appeal Under 37 C.F.R. § 41.37

Attn: Mail Stop: Appeal Brief-Patents

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal from the final rejection of claims 1-4, 6, 14-17, 19, 28, 29, and 32-42 for the above-captioned U.S. Patent Application was filed on December 26, 2007, appealing the decision of the Examiner in the Final Office Action mailed July 25, 2007, maintaining the rejection of claims 1-4, 6, 14-17, 19, 28, 29, and 32-42. In support of the Notice of Appeal, Appellant hereby files an appeal brief as required under 37 C.F.R. § 41.37(a). Appellant has also filed herewith the fee for filing a brief in support of an appeal as set forth in 37 C.F.R. § 41.37(a)(2).

TABLE OF CONTENTS

I. Real Party in Interest (37 C.F.R. § 41.37(c)(1)(i))

The real party of interest is Broadcom Corporation, having its principal place of business at 5300 California Avenue, Irvine, California, 92617. An assignment assigning all right, title, and interest in and to the patent application from the inventors to Broadcom was recorded in the U.S. Patent & Trademark Office on July 11, 2003 at Reel 014283, Frame 0907.

II. Related Appeals and Interferences (37 C.F.R. § 41.37(c)(1)(ii))

To the best of knowledge of Appellants, Appellants' legal representative, and Appellants' assignee, there are no other appeals or interferences which will directly affect or be directly affected or have a bearing on the Board's decision in the pending appeal.

III. Status of the Claims (37 C.F.R. § 41.37(c)(1)(iii))

This application was originally filed as U.S. Application No. 10/617,538 on July 11, 2003 claiming benefit to U.S. Provisional Application No. 60,437,538 filed on December 31, 2002. The originally filed application had 31 claims. In the Amendment and Reply filed on April 27, 2007, claims 1, 14, and 28 were amended, claims 5, 7-13, 18, 20-27, 30, and 31 were cancelled, and new claims 32-42 were added.

The pending claims were finally rejected in an Office Action mailed July 25, 2007. No claim stands allowed.

Accordingly, the claims on appeal are claims 1-4, 6, 14-17, 19, 28, 29, and 32-42. A copy of the claims on appeal can be found in the attached Appendix as required under 37 C.F.R. § 41.37(c)(1)(viii).

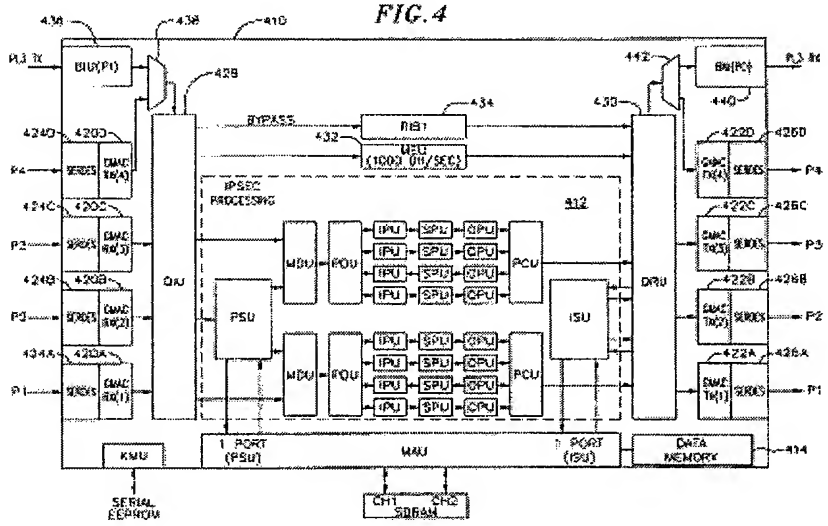
IV. Status of Amendments (37 C.F.R. § 41.37(c)(1)(iv))

All amendments have been entered. The Final Office Action dated July 25, 2007, responded to and acknowledged Appellants' amendment filed April 27, 2007.

V. Summary of the Claimed Subject Matter (37 C.F.R. § 41.37(c)(1)(v))

The invention as recited in independent claims 1, 14, 28, and 39 includes a "flexible mechanism that allows each packet [received by a security processor] to be classified into an established flow." (¶0094, lines 10-11)1. FIG. 4, reproduced below, depicts an exemplary security processor 410.

FIG. 4



Security processor 410 includes a plurality of Gigabit Media Access Controllers (GMAC) for receiving data packets (GMAC Rx 420A-D) and for transmitting data packets (GMAC Tx 422A-D). On the receive side, security processor 410 includes a data input unit (DIU) 428 coupled to the plurality of receiver GMACs 420A-D. DIU 428 "manages packet flow from the receiver inputs into the processing of the Gigabit security processor 410 and may extract and process header information ... Packets may be routed to a public key processing component 432. Packets also may be routed to an IPSec processing component 412 based, for example, on analysis of packet header information ..." (¶0060, lines 1-11). As illustrated in FIG. 4, the IPsec processing component 412 includes a policy lookup unit (PSU) coupled to a plurality of merge

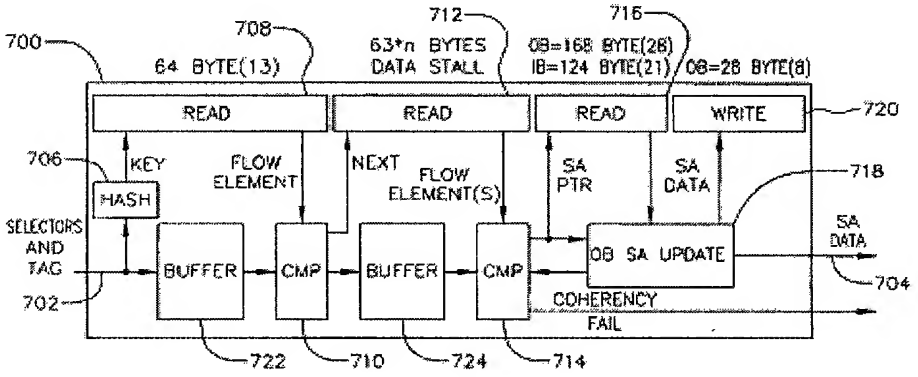
---

[1] For ease of discussion, citations herein are based on the publication of Appellants' specification, U.S. Patent Publication No. 2004/0128553.

data units (MDU). Each MDU is coupled to a packet distribution unit (PDU) which is in turn coupled to a plurality of security processing units (SPU). The plurality of security processing units (SPU) are coupled via an output processing unit (OPU) to a packet convergence unit (PCU). (*See* ¶0126, lines 1-7).

FIG. 7, reproduced below, depicts an embodiment of the policy lookup unit (PSU) 700.

FIG. 7



During processing, the "PSU block receives a set of selectors in the SAHandle [Security Association Handle] from the DIU along with the MCW [management control word]. The PSU hashes the selectors to generate an address unless the address is provided directly." (¶0097, lines 1-4). The resulting address "is used to read the flow element from a hash table (different base address for separate hash tables). The flow element contains one or more flow entries with selectors that are used to match the original packet selectors." (¶0098, lines 1-5).

A flow has a well-understood and standardized meaning for IPSec implementations. The definition of a flow, as would have been understood by a person of skill in the art, can be found in the IPv6 Flow Label Specification published by the Internet Engineering Task Force (IETF), a "flow is a sequence of packets sent from a particular source to a particular unicast, anycast or multicast destination that the source desires to label as a flow. A flow could consist of all packets in a specific transport connection or a media stream. However, a flow is not necessarily

1:1 mapped to a transport connection." (IETF INTERNET DRAFT, IPv6 Flow Label Specification, April 2003).

Upon receipt of the flow element, a "compare unit 710 in the PSU compares the selectors to the ones found in the flow entries in sequential order. If the selectors are not found within the base flow element, the rest of the flow elements are also searched in order until a match is found. If no match is found, the packet is flagged with an error 2." (¶0099, lines 1-7). Each flow entry includes a pointer to a Security Association data structure. After "the selectors have been resolved (i.e., the flow is found), the PSU compare block 714 fetches the SA Data Structure from the SA_PTR location in the flow entry with matching selectors." (¶0101, lines 1-4).

Thus, as recited in the independent claims, the policy lookup unit identifies a flow based on the received Security Association handle prior to retrieving a security association. As described above, and recited in independent claims 1, 14, and 39, the flow is identified in a series of steps. First, a first flow element including a plurality of flow entries is retrieved using the flow element address. A determination is then made whether a selector received in the secuirty association handle is present in one of the flow entries in the retrieved first flow element. If a selector received in the security handle is not present in one of the flow entries in the retrieved first flow element, the remaining flow elements are retrieved.

Upon receipt of the SA Data Structure, the security processor then "prepends the SA Data Structure (MCW, SAUpdate, SAData, Outer IP Header, Security Header, etc.) to the front of the packet." (¶0064, lines 3-5). "The combination of the prepended SA Data Structure and the original packet are merged to construct a packet." (¶0065, lines 1-2). The "resulting packet stream 506 contains all of the information required to completely process the packet for an IPSec operation." (¶0066, lines 1-2).

VI. Grounds of Rejection to be Reviewed on Appeal (37 C.F.R. § 41.37(c)(1)(vi))

In the final Office Action mailed July 25, 2007, the Examiner rejected claims 1-4, 6, 14-17, 19, 28, 29, and 32-42 under 35 U.S.C. §102(e) as allegedly being anticipated over Noehring *et al.*, U.S. Patent Publication No. 20020188838 (hereinafter Noehring).

Accordingly, the grounds of rejection to be reviewed on appeal are:

> Whether claims 1-4, 6, 14-17, 19, 28, 29, and 32-42 under 35 U.S.C. §102(e) are unpatentable over U.S. Patent Publication No. 20020188838 to Noehring, *et al.*

VII. Argument (37 C.F.R. § 41.37(c)(1)(vii))

1. The Examiner's Anticipation Rejection

A Final Office Action was mailed on July 25, 2007. Claims 1-4, 6, 14-17, 19, 28, 29, and 32-42 were rejected under 35 U.S.C. §102(e) over U.S. Patent Publication No. 20020188838 to Noehring, *et al* (Noehring). Appellants' remarks focus mainly on independent claims 1, 14, 28, and 39 because any claim which depends from a patentable independent claim is also patentable by virtue of its dependency.

2. The Anticipation Rejection is in Error and Must be Reversed

To establish a *prima facie* case of anticipation under §102(e), the Examiner must show that "each an every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). Because the Examiner has failed to establish that each and every element of independent claims 1, 14, 28, and 39 is described in Noehring, the rejection of claims claims 1-4, 6, 14-17, 19, 28, 29, and 32-42 must be reversed.

Noehring fails to disclose the identification of a flow entry (flow) associated with a packet and retrieval of the security association for the identified flow. In the Office Action, the Examiner appears to equate a flow entry to a channel in Noehring. (Final Office Action, p. 4)("see Noehring paragraph [0052], lines 1-4: channel (flow entry) selected for packet"). Appellants' respectfully disagree with this understanding.

As described above, a flow is associated with a connection between a source and a destination. (*See* IETF INTERNET DRAFT, IPv6 Flow Label Specification)("flow is a sequence of packets sent from a particular source to a particular unicast, anycast or multicast destination that the source desires to label as a flow."). In Noehring, a channel is associated with a processing core in the crypto core engine. (*See e.g.,* Noehring, ¶0036, lines 1-2) ("A plurality of independent channels are preferably used to process many independent packets concurrently."). A channel is associated with internal processing and is not related to the source and destination pair for a packet. Thus, a channel is not equivalent to a flow entry (flow).

Further, the process used to retrieve a Security Association in Noehring is very different than the process recited in Appellants' independent claims. FIG. 1 of Noehring, reproduced below, depicts "a simplified functional block diagram of a system architecture suitable for use in implementing the preferred embodiments of the present invention." (Noehring, ¶0027, lines 1-3).

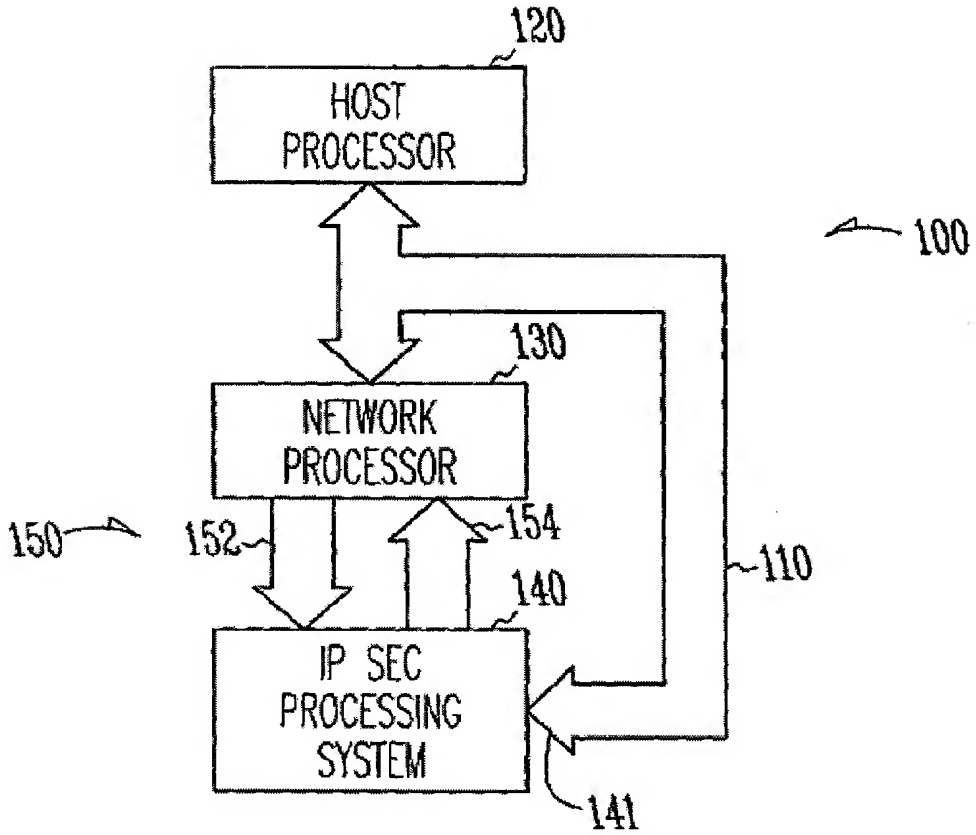


Fig. 1

In Noehring, for outbound packets, the network processor 130 performs a security policy look-up and prepends a security association database (SAD) entry address to a packet. (Noehring, ¶0051). The security association is then read into memory by the IP Sec processing system 140 using the SAD entry address. (Noehring, ¶0053). In Noehring, for inbound packets, the IP Sec processing system 140 identifies a security policy index value having a pointer pointing to the SAD entry. (Noehring, ¶0067). The IP Sec processing system 140 reads at least a portion of the security association into a local buffer using the identified pointer. (Noehring, ¶0068). Noehring does not retrieve a block of security association entries. Noehring instead retrieves a single security association stored at the address provided. Furthermore, in Noehring, "the SAD entry address is verified by comparing the SAD entry address prepended to the data

packet with valid SAD addresses. If the SAD entry is invalid, the packet is dropped (step 810) and an error is logged (step 812)." (Noehring, ¶0054, lines 1-4). Noehring does not describe retrieving additional entries if the initial retrieved entry cannot be verified.

Accordingly, Noehring fails to teach each and every feature of independent claims 1, 14, 28, and 39. Specifically, Noehring does not teach or suggest a method including:

> receiving a security association handle for each packet in the plurality of packets, wherein the security association handle includes a set of selectors;
> for each packet, identifying a flow entry for the packet, including:
> determining a flow element address for the packet,
> retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries,
> determining whether a selector in the set of security association handle selectors is present in one of the plurality of flow entries, and
> retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries;
> retrieving security association information for each packet using the identified flow entry

as recited in independent claims 1 and 14. Noehring also does not teach or suggest a system including:

> a cryptographic processing module, wherein the cryptographic processing module includes:
> a policy lookup unit configured to identify a flow associated with each of the received plurality of packets and to retrieve a security association for each identified flow;
> a merge data unit coupled to the policy lookup unit configured to merge a portion of the security association retrieved by the policy lookup unit with the associated packet,
> a plurality of cryptographic processors, each coupled to the merge data unit for performing cryptographic operations on the merged packets.

as recited in independent claim 28. Noehring further does not teach or suggest:

> determining a flow element address for the packet;
> retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries;
> identifying a flow entry having a selector matching a selector in the set of security association handle selectors;

retrieving security association information using the identified flow entry

as recited in independent claim 39.

For at least the foregoing reasons, independent claims 1, 14, 28, and 39 and their respective dependent claims 2-4, 6, 15-17, 19, 29, 32-38, and 40-42 are patentable over Noehring and the rejection of claims 1-4, 6, 14-17, 19, 28, 29, and 32-42 must be reversed.

VIII. Conclusion

Claims 1-4, 6, 14-17, 19, 28, 29, and 32-42 are patentable over Noehring because the Examiner has failed to establish that Noehring anticipates these claims. Therefore, Appellants respectfully request that the Board reverse the Examiner's final rejection of these claims and remand this application for issue.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

for 35,613
Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

Date: 4/28/08

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

CLAIMS APPENDIX

1. (previously presented) A packet processing method comprising:

receiving a plurality of packets;

receiving a security association handle for each packet in the plurality of packets, wherein the security association handle includes a set of selectors;

for each packet, identifying a flow entry for the packet, including:

determining a flow element address for the packet,

retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries,

determining whether a selector in the set of security association handle selectors is present in one of the plurality of flow entries, and

retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries;

retrieving security association information for each packet using the identified flow entry;

generating header information for each of the plurality of packets;

adding the header information to each of the plurality of packets to generate encapsulated packets; and

distributing the encapsulated packets to a plurality of cryptographic processors.

2. (original) The method of claim 1 wherein the information comprises one or more of the group consisting of sequence number and byte count.

3. (original) The method of claim 1 wherein the encapsulated packets comprise IPsec packets.

4. (original) The method of claim 1 wherein packets are encapsulated on a per-packet basis.

5. (canceled).

6. (original) The method of claim 1 wherein the packets are received from a host processor.

7-13. (canceled)

14. (previously presented) A packet processing method comprising:

receiving a plurality of packets comprising header information and encrypted data;

receiving a security association handle for each packet in the plurality of packets, wherein the security association handle includes a set of selectors;

for each packet, identifying a flow entry for the packet, including:

determining a flow element address for the packet,

retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries,

determining whether a selector in the set of security association handle selectors is present in one of the plurality of flow entries, and

retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries;

retrieving security association information for each packet using the identified flow entry;

distributing the packets to a plurality of cryptographic processors;

decrypting the encrypted portion of each packet based on a portion of the security association information retrieved for the packet;

modifying, by a common processing component, at least a portion of the header information of the decrypted packets; and

transmitting the decrypted packets.

15. (original) The method of claim 14 wherein the at least a portion of the header information comprises one or more of the group consisting of sequence number and byte count.

16. (original) The method of claim 14 wherein the encrypted packets comprise IPsec packets.

17. (original) The method of claim 14 wherein the at least a portion of the header information is modified on a per-packet basis.

18. (canceled).

19. (original) The method of claim 14 wherein the packets are transmitted to a host processor

20 - 27. (canceled)

28. (previously presented) A packet processing system comprising:

at least one media access controller for receiving a plurality of packets;

at least one data memory for storing security association information; and

a cryptographic processing module, wherein the cryptographic processing module includes:

a policy lookup unit configured to identify a flow associated with each of the received plurality of packets and to retrieve a security association for each identified flow;

a merge data unit coupled to the policy lookup unit configured to merge a portion of the security association retrieved by the policy lookup unit with the associated packet,

a plurality of cryptographic processors, each coupled to the merge data unit for performing cryptographic operations on the merged packets.

29. (original) The packet processing system of claim 28 wherein the at least a portion of the security association information comprises one or more of the group consisting of sequence number and byte count

30-31. (canceled)

32. (previously presented) The method of claim 1, wherein determining a flow element address includes:

hashing the selectors in the set of security association handle selectors to generate the flow element address.

33. (previously presented) The method of claim 1, wherein the step of determining a flow element address includes:

retrieving a security parameter index from the set of security association handle selectors; and

using the retrieved security parameter index as the flow element address.

34. (previously presented) The method of claim 1, further comprising:

processing each encapsulated packet based on the retrieved security association information for the packet; and

transmitting the processed packet.

35. (previously presented) The method of claim 1, further comprising:

modifying a least a portion of the retrieved security association information; and

generating header information for the packets including a portion of the modified security association information.

36. (previously presented) The method of claim 14, wherein determining a flow element address includes:

hashing the selectors in the set of security association handle selectors to generate the flow element address.

37. (previously presented) The method of claim 14, wherein the step of determining a flow element address includes:

retrieving a security parameter index from the set of security association handle selectors; and

using the retrieved security parameter index as the flow element address.

38. (previously presented) The packet processing system of claim 28, wherein the cryptographic processing module further comprises:

a distributor coupled between the merge data unit and the plurality cryptographic processors for distributing merged packets to the plurality of cryptographic processors.

39. (previously presented) A method for determining security association information in a cryptographic processor comprising:

receiving a security association handle for a packet, wherein the security association handle includes a set of selectors;

determining a flow element address for the packet;

retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries;

identifying a flow entry having a selector matching a selector in the set of security association handle selectors;

retrieving security association information using the identified flow entry; and

transmitting at least a portion of the retrieved security association information to a cryptographic processing engine.

40. (previously presented) The method of claim 39, further comprising:

retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries

41. (previously presented) The method of claim 39, wherein determining a flow element address includes:

hashing the selectors in the set of security association handle selectors to generate the flow element address.

42. (previously presented) The method of claim 39, wherein the step of determining a flow element address includes:

retrieving a security parameter index from the set of security association handle selectors; and

using the retrieved security parameter index as the flow element address.

X. Evidence Appendix (37 C.F.R. § 41.37(c)(1)(ix))

None

XI. Related Proceedings Appendix (37 C.F.R. § 41.37(c)(1)(x))

None